PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-212458
(43)Date of publication of application : 06.08.1999

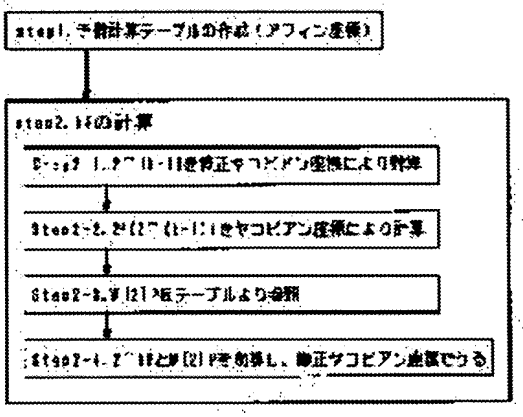
(51)Int.Cl. G09C 1/00
G09C 1/00
G09C 1/00
H04L 9/30

(21)Application number : 10-013748
(22)Date of filing : 27.01.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MIYAJI MITSUKO
ONO TAKATOSHI

(54) ELLIPTIC CURVE OPERATION DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an elliptic curve operation device in a quick cipher and signature system.
SOLUTION: In an auxiliary calculation table generation step 1, an auxiliary calculation table is generated with affine coordinates. In a kP calculation step 2, kP is obtained by mixture coordinates where addition to values (affine coordinates) of the auxiliary calculation table is obtained in revised Jacobian coordinates and the result is multiplied by power of two in correction Jacobian coordinates but the final result is obtained in Jacobian coordinates. Mixture coordinates and revised Jacobian coordinates are used to reduce the number of multiplications.



LEGAL STATUS

[Date of request for examination] 19.01.2005
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－212458

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６５０	Ｇ０９Ｃ	1/00	６５０Ｚ
		６２０			６２０Ｚ
		６４０			６４０Ｂ
Ｈ０４Ｌ	9/30		Ｈ０４Ｌ	9/00	６６３Ｚ

審査請求　未請求　請求項の数10　ＯＬ　（全９頁）

(21)出願番号　特願平10－13748

(22)出願日　平成10年(1998)１月27日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

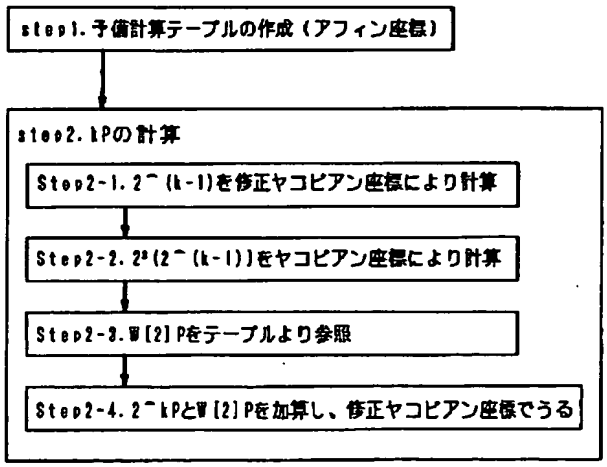
(72)発明者　宮地　充子
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　小野　貴敏
愛知県名古屋市中区栄２丁目６番１号白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内

(74)代理人　弁理士　掩本　智之　（外１名）

(54)【発明の名称】　楕円曲線演算装置

(57)【要約】
【課題】　高速な暗号及び署名方式における楕円曲線の演算装置を提供する。
【解決手段】(1)予備計算テーブル作成
アフィン座標で予備計算テーブルを作成する。
(2) kP の計算
予備計算テーブルの値(アフィン座標）との加算を修正ヤコビアン座標で求めて、その結果を修正ヤコビアン座標で2冪倍するが、最終結果はヤコビアン座標で得るという混合座標によりkPを求める。混合座標と修正ヤコビアン座標を利用することで、乗算全体の回数を削減することを特徴とする楕円曲線演算装置を構成する。



【特許請求の範囲】

【請求項１】pを素数とし、有限体GF(p)上の楕円曲線をE:y^2=x^3+ax+b とし、E(GF(p)) の元 P = (x,y) を Z=1, X=x*Z^2, Y=y*Z^3 により変換した射影座標 (X,Y,Z) において、加算公式の内部点を修正ヤコビアン座標(X,Y,Z,a*Z^4)ともつことを特徴とする楕円曲線演算装置。

【請求項２】pを素数とし、rを正整数とするとき、有限体GF(p^r)上の楕円曲線を E とし、E(GF(p^r)) の元を P = (x,y) を Z=1, X=x*Z^2, Y=y*Z^3 により変換した射影座標 (X,Y,Z) において、加算公式の内部点を修正ヤコビアン(X,Y,Z,a*Z^4)ともつことを特徴とする楕円曲線演算装置。

【請求項３】上記楕円曲線演算装置において、E(GF(p)) の元を修正ヤコビアン座標

P=(X1, Y1, Z1, a*Z1^4), Q=(X2, Y2, Z2, a*Z2^4) (P ≠ Q)

で表すとき、P+Q=R=(X3, Y3, Z3, a*Z3^4)を、

U1=X1*Z2^2, U2=X2*Z1^2, S1=Y1*Z2^3, S2=Y2*Z1^3, H=U2-U1, r=S2-S1

を計算し、

X3 = -H^3 -2U1*H^2+ r^2,

Y3 = -S1*H^3 + r(U1*H^2 -X3),

Z3 = Z1*Z2*H,

a*Z3^4 = a(Z3^2)^2

により求めることを特徴とした請求項１記載の楕円曲線演算装置。

【請求項４】上記楕円曲線演算装置において、E(GF(p)) の元を、修正ヤコビアン座標

P=(X1, Y1, Z1, a*Z1^4)

とするとき、2P=R=(X3, Y3, Z3, a*Z3^4)を,

S=4X1*Y1^2, M=3X1^2+a*Z1^4, T=-2S+M^2

を計算し,

X3 = T,

Y3 = -8Y1^4 + M(S-T),

Z3 = 2Y1*Z1,

a*Z3^4 = 2^4*(Y1^4)*(a*Z1^4)

により求めることを特徴とした請求項１記載の楕円曲線演算装置。

【請求項５】pを素数とし、kを正整数とするとき、有限体 GF(p) 上の楕円曲線を

E:y^2=x^3+ax+b

とし、E(GF(p)) の元 P = (x,y) の冪倍点 kP = P + ... + P(k回の加算)の計算を、座標を２個以上組み合わせて行なうことを特徴とした楕円曲線演算装置。

【請求項６】pを素数とし、r,k を正整数とし、有限体GF(p^r)上の楕円曲線をEとし、E(GF(p^r)) の元 P = (x,y) の冪倍点 kP = P + ... + P(k回の加算)の計算を、座標を２個以上組み合わせて行なうことを特徴とした楕円曲線演算装置。

【請求項７】pを素数、kを正整数、有限体GF(p)上の楕円曲線をE:y^2=x^3+ax+b とし、

E(GF(p)) の元 P = (x,y) の冪倍点 kP = P + ... + P (k回の加算)

を計算する上記楕円曲線演算装置において、wを正整数とし、kを

k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1])・・・)+W[0])

(W[i] は奇数, かつ1 ≦ W[i] ≦ 2^w-1)と表すとき、テーブル

iP = Pi=(xi,yi) (i は奇数, かつ 1 ≦ i ≦ 2^w-1)

をアフィン座標で計算し、kP の計算を、(ki-1) 回の2倍点の計算は、請求項１記載の座標 (X, Y, Z, a*Z^4) で行い、ki 回目の２倍点の結果は、ヤコビアン座標 (X, Y, Z) で求め、(X,Y,Z)とテーブルの点 Piとの加算は、請求項１記載の座標 (X, Y, Z, a*Z^4)で求めることを、繰り返すことによって得ることを特徴とした請求項５記載の楕円曲線演算装置。

【請求項８】pを素数、kを正整数、有限体GF(p)上の楕円曲線をE:y^2=x^3+ax+b とし、

E(GF(p)) の元 P = (x,y) の冪倍点 kP = P + ... + P (k回の加算)

を計算する上記楕円曲線演算装置において、wを正整数とし、kを

k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1])・・・)+W[0])

(W[i] は奇数, かつ1 ≦ W[i] ≦ 2^w-1)と表すとき、テーブル

iP = Pi=(Xi,Yi,Zi,Zi^2,Zi^3)　(i は奇数, かつ 1 ≦ i ≦ 2^w-1)

をチャドノブスキヤコビアン座標で求め、kP の計算を、(ki-1) 回の2倍点の計算は、請求項１記載の修正ヤコビアン座標 (X, Y, Z, a*Z^4) で行い、ki 回目の２倍点の結果は、ヤコビアン座標 (X,Y, Z)で求め、(X,Y,Z)とテーブルの点 Piとの加算は、請求項１記載の修正ヤコビアン座標(X, Y, Z, a*Z^4)で求めることを、繰り返すことによって得ることを特徴とした請求項５記載の楕円曲線演算装置。

【請求項９】pを素数、kを正整数、有限体GF(p)上の楕円曲線をE:y^2=x^3+ax+b とし、

E(GF(p)) の元 P = (x,y) の冪倍点 kP = P + ... + P (k回の加算)

を計算する上記楕円曲線演算装置において、wを正整数とし、kを

k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1])・・・)+W[0])

(W[i] は奇数, かつ1 ≦ W[i] ≦ 2^w-1)と表すとき、テーブル

iP = Pi=(Xi,Yi,Zi,Zi^2,Zi^3)

(i は奇数, かつ 1 ≦ i ≦ 2^w-1)をチャドノブスキヤコビアン座標で求めるとき、はじめに、2P=(x,y) をアフィン座標で求めることを特徴とした請求項８記載の楕円曲線演算装置。

【請求項１０】pを素数、kを正整数、有限体GF(p)上の楕円曲線をE:y^2=x^3+ax+b とし、
E(GF(p)) の元 P = (x,y) の冪倍点 kP = P + ... + P (k回の加算)
を計算する上記楕円曲線演算装置において、wを正整数とし、kを
k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1])・・・)+W[0])
(W[i] は奇数，かつ1 ≦ W[i] ≦ 2^w-1)と表すとき、テーブル
iP = Pi=(Xi,Yi,Zi,Zi^2,Zi^3)
(i は奇数，かつ 1 ≦ i ≦ 2^w-1)をチャドノブスキヤコビアン座標で求めるとき、はじめに、2P=(x,y) をチャドノブスキヤコビアン座標で求めることを特徴とした請求項８記載の楕円曲線演算装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は情報セキュリテイ技術としての暗号技術に関するものであり、特に、楕円曲線を用いて実現する暗号及びデジタル署名技術に関するものである。

【０００２】

【従来の技術】秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。この署名方式には公開鍵暗号とよばれる暗号方式を用いる。公開鍵暗号は通信相手が多数の時、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、多数の通信相手と通信を行なうのに不可欠な基盤技術である。簡単に説明すると、これは暗号化鍵と復号化鍵が異なり、復号化鍵は秘密にするが、暗号化鍵を公開する方式である。この公開鍵暗号の安全性の根拠に用いられるものに離散対数問題がある。離散対数問題には代表的に、有限体上定義されるもの及び楕円曲線上定義されるものがある。これはニイルコブリッツ著 ”ア コウス イン ナンバア セオリイ アンド クリプトグラヒイ” (Neal Koblitz , ” A Course in Number theory and Cryptography”, Spinger-Verlag,1987)に詳しく述べられている。楕円曲線上の離散対数問題を以下に述べる。

【０００３】楕円曲線上の離散対数問題
E(GF(p)) を有限体GF(p)上定義された楕円曲線Eとし、Eの位数が大きな素数で割れる元Gをベースポイントとする。このとき、Eの与えられた元Yに対して、
Y=xG
となる整数xが存在するならばxを求めよ。

【０００４】以下に上記楕円曲線上の離散対数問題を応用したエルガマル署名をまず述べる。

【０００５】（従来例１）図６は従来例である楕円曲線上のエルガマル署名方式の構成をしめすものである。

【０００６】以下同図を参照しながら従来例の手順を説明する。
(1) センタの設定
pを素数、GF (p) 上の楕円曲線をEとし、その素数位数qの元をGとする。ユーザＡの公開鍵をYa=xaGとし、秘密鍵をxaとする。センターは素数p及び楕円曲線E及びベースポイントGをシステムパラメータとして公開するとともに、Ａの公開鍵Yaを公開する。

【０００７】(2) 署名生成
１ 乱数ｋを生成する。

【０００８】２ R1=kG=(rx,ry)
sk = m + rxxa (mod q) を計算する
３ (R1、ｓ）を署名としてｍとともに送信する。

【０００９】(3) 署名検証
s1 = mG + rxYa
が成り立つかチェックする。

【００１０】上記従来例１でわかるように、楕円曲線を用いた署名方式では、固定点Ｇの冪倍の演算 kG 及び任意点 P(従来例では公開鍵Yaに相当)の冪倍の演算 kPaの計算が必要である。このうち、固定点の演算は、以下の文献に知られるように、予めテーブルを用意しておくことが可能なので、高速に実現できる。

【００１１】E. F. Brickell, D.M. Gordon, K. S. McCurley and D.B. Wilson”Fast exponentiation with precomputation”,Advances in cryptology-proceedings of Eurocrypt'92,Lecture notes in computer science, 1993, Springer-verlag, 200-207.一方、任意点Ｐの冪倍を計算する方法であるが、これは以下の文献が詳しい。

【００１２】Miyaji, Ono, and Cohen,”Efficient elliptic curve exponentiation”,Advances in cryptology-proceedings of ICICS'97,Lecture notes in computer science, 1997, Springer-verlag, 282-290.ここで簡単に、この従来例について説明する。

【００１３】図７は従来例である楕円曲線演算装置の構成を示すものである。以下同図を参照しながら従来例の手順を説明する。

【００１４】（従来例２）pを160ビットの素数とし、有限体GF(p)上の楕円曲線を E とし、E(GF(p)) の任意の元 P に対して、 k*P の計算をする。ここで、kの２進表現を、
k = k0 + k1*2+ k2*2^2 + ・・・ + k159*16^159=[k159,.....,k2,k1,k0]
(k0,・・・,k159 = 0,1) とする。

【００１５】step1. ウインドウ幅 w=4 をもつ addition-subtraction 表現への変換
k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1])・・・)+W[0])
ここで、W[i] は奇数，かつ1 ≦ W[i] ≦ 2^4-1 である。

【００１６】W[i] への変換方法は、奇数 0 ≦ t ≦ 2^5-1 を -2^4+1 ≦ t ≦ 2^4-1に変換する自然な変換で

ある。

【００１７】step2. 予備計算テーブルの作成

sP(s=3,5,...,15)をヤコビアン座標で計算し、予備計算テーブルとする。

【００１８】step3. kP の計算

Tを上位ビットより探索し、ウインドウがある毎に、予備計算テーブルの値との加算をヤコビアン座標で求めて、その結果をヤコビアン座標で2冪倍することを繰り返す。

【００１９】従来例では、一つの座標を利用するため全体の乗算回数が多くなるという問題がある。

【００２０】トータルの計算量を乗算回数で表すと、1882Mul になる。ここで、Mul は１回のGF(p)での乗算を表す。任意点の冪倍点の演算は、２倍点の演算が加算に比べて数多く必要になる。ところが、従来利用されていたプロジェクティブ座標、ヤコビアン座標、チャドノブスキヤコビアン座標の２倍点は、必要な乗算回数が多いので、kPの計算の全体の計算量が大きくなるという問題がある。

【００２１】

【発明が解決しようとする課題】楕円曲線を用いた暗号方式や署名方式では、固定点の冪倍点や任意点の冪倍点を求める楕円曲線演算装置が必須である。特に、任意点の冪倍点の演算には、時間がかかるので、これを高速に行なう研究がされている。

【００２２】従来例の冪倍点を求める方法は、各座標系を用いた際のトータルの計算量が最も小さくなる座標を一つだけ利用する方法で、トータルの乗算回数が多いという欠点がある。

【００２３】本発明は、この従来例における問題点を鑑みて行なわれたもので、楕円曲線の加算、２倍点の計算時間を鑑みて、楕円曲線演算装置を構成し、これにより高速な暗号及び署名方式を提供することを目的とする。

【００２４】

【課題を解決するための手段】本発明は上述の問題点を解決するため、請求項１ではp を素数とし、有限体GF(p)上の楕円曲線を E:y^2=x^3+ax+b とし、E(GF(p)) の元を P = (x,y) を Z=1, X=x*Z^2, Y=y*Z^3 により変換した射影座標 (X,Y,Z) において、加算公式の内部点を修正ヤコビアンを特徴とする楕円曲線演算装置としている。

【００２５】請求項２では、pを素数とし、rを正整数とするとき、有限体GF(p^r)上の楕円曲線を E とし、E(GF(p^r)) の元を

P = (x,y) を Z=1, X=x*Z^2, Y=y*Z^3

により変換した射影座標 (X,Y,Z) において、加算公式の内部点を修正ヤコビアンを特徴とする楕円曲線演算装置としている。

【００２６】請求項３では、上記楕円曲線演算装置において、E(GF(p)) の元を修正ヤコビアン座標

P=(X1, Y1, Z1, a*Z1^4), Q=(X2, Y2, Z2, a*Z2^4) (P ≠ Q)

で表すとき, P+Q=R=(X3, Y3, Z3, a*Z3^4)を、

U1=X1*Z2^2, U2=X2*Z1^2, S1=Y1*Z2^3, S2=Y2*Z1^3, H=U2-U1, r=S2-S1

を計算し、

X3 = -H^3 -2U1*H^2+ r^2,

Y3 = -S1*H^3 + r(U1*H^2 -X3),

Z3 = Z1*Z2*H,

a*Z3^4 = a(Z3^2)^2

により求めることを特徴とした請求項１記載の楕円曲線演算装置としている。

【００２７】請求項４では、上記楕円曲線演算装置において、E(GF(p)) の元を、修正ヤコビアン座標

P=(X1, Y1, Z1, a*Z1^4)

とするとき、2P=R=(X3, Y3, Z3, a*Z3^4)を、

S=4X1*Y1^2, M=3X1^2+a*Z1^4, T=-2S+M^2

を計算し、

X3 = T,

Y3 = -8Y1^4 + M(S-T),

Z3 = 2Y1*Z1,

a*Z3^4 = 2^4*(Y1^4)*(a*Z1^4)

により求めることを特徴とした請求項１記載の楕円曲線演算装置としている。

【００２８】請求項５では、pを素数とし、kを正整数とするとき、有限体 GF(p) 上の楕円曲線を

E:y^2=x^3+ax+b

とし、

E(GF(p)) の元 P = (x,y) の冪倍点 kP = P + ... + P (k回の加算)

の計算を、座標を２個以上組み合わせて行なうことを特徴とした楕円曲線演算装置を特徴とする楕円曲線演算装置としている。

【００２９】請求項６では、p を素数とし、r,k を正整数とし、有限体GF(p^r)上の楕円曲線を E とし、E(GF(p^r)) の元 P = (x,y) の冪倍点 kP = P + ... + P(k回の加算)の計算を、座標を２個以上組み合わせて行なうことを特徴とした楕円曲線演算装置としている。

【００３０】請求項７では、pを素数、kを正整数、有限体GF(p)上の楕円曲線をE:y^2=x^3+ax+b とし、

E(GF(p)) の元 P = (x,y) の冪倍点 kP = P + ... + P (k回の加算)

を計算する上記楕円曲線演算装置において、wを正整数とし、kを

k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1])・・・)+W[0])

(W[i] は奇数, かつ1 ≦ W[i] ≦ 2^w-1)と表すとき、テーブル

iP = Pi=(xi,yi) (i は奇数, かつ 1 ≦ i ≦ 2^w-1)

をアフィン座標で計算し、kP の計算を、(ki-1) 回の2倍点の計算は、請求項１記載の座標 (X, Y, Z, a*Z^4)

で行い、ki 回目の２倍点の結果は、ヤコビアン座標(X, Y, Z) で求め、(X,Y,Z)とテーブルの点 Piとの加算は、請求項１記載の座標 (X, Y, Z, a*Z^4)で求めることを、繰り返すことによって得ることを特徴とした請求項５記載の楕円曲線演算装置としている。

【００３１】請求項８では、p を素数、kを正整数、有限体GF(p)上の楕円曲線を

E:y^2=x^3+ax+b

とし、E(GF(p)) の元 P = (x,y) の冪倍点 kP = P + ... + P(k回の加算)を計算する上記楕円曲線演算装置において、wを正整数とし、kを

k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1])・・・)+W[0])

(W[i] は奇数, かつ1 ≦ W[i] ≦ 2^w-1)と表すとき、テーブル

iP = Pi=(Xi,Yi,Zi,Zi^2,Zi^3) (i は奇数, かつ 1 ≦ i ≦ 2^w-1)

をチャドノブスキヤコビアン座標で求め、kP の計算を、(ki-1) 回の2倍点の計算は、請求項１記載の修正ヤコビアン座標(X, Y, Z, a*Z^4) で行い、ki 回目の２倍点の結果は、ヤコビアン座標 (X, Y, Z)で求め、(X,Y,Z)とテーブルの点 Piとの加算は、請求項１記載の修正ヤコビアン座標(X, Y, Z, a*Z^4)で求めることを、繰り返すことによって得ることを特徴とした請求項５記載の楕円曲線演算装置としている。

【００３２】請求項９では、pを素数、kを正整数、有限体GF(p)上の楕円曲線をE:y^2=x^3+ax+b とし、E(GF(p)) の元 P = (x,y) の冪倍点 kP = P + ... + P(k回の加算)

を計算する上記楕円曲線演算装置において、wを正整数とし、kを

k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1])・・・)+W[0])

(W[i] は奇数, かつ1 ≦ W[i] ≦ 2^w-1)と表すとき、テーブル

iP = Pi=(Xi,Yi,Zi,Zi^2,Zi^3) (i は奇数, かつ 1 ≦ i ≦ 2^w-1)

をチャドノブスキヤコビアン座標で求めるとき、はじめに、2P=(x,y) をアフィン座標で求めることを特徴とした請求項８記載の楕円曲線演算装置としている。

【００３３】請求項１０では、pを素数、kを正整数、有限体GF(p)上の楕円曲線をE:y^2=x^3+ax+b とし、E(GF(p)) の元 P = (x,y) の冪倍点 kP = P + ... + P(k回の加算)

を計算する上記楕円曲線演算装置において、wを正整数とし、kを

k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1])・・・)+W[0])

(W[i] は奇数, かつ1 ≦ W[i] ≦ 2^w-1)と表すとき、テーブル

iP = Pi=(Xi,Yi,Zi,Zi^2,Zi^3) (i は奇数, かつ 1 ≦ i ≦ 2^w-1)

をチャドノブスキヤコビアン座標で求めるとき、はじめに、2P=(x,y) をチャドノブスキヤコビアン座標で求めることを特徴とした請求項８記載の楕円曲線演算装置としている

【００３４】

【発明の実施の形態】以下、本発明の実施の形態について図を用いて説明する。

【００３５】（実施の形態１）図１は楕円曲線演算装置における修正ヤコビアンによる加算点の方法を示すものである。以下同図を参照しながら加算方法を説明する。

【００３６】ここでは、pを160ビットの素数とし、GF(p)上の楕円曲線 E:y^2 = x^3 +ax+b, その元を P=(X1, Y1, Z1, a*Z1^4), Q=(X2, Y2, Z2, a*Z2^4) (P ≠ Q)で表すとき、

P+Q = R= (X3, Y3, Z3, a*Z3^4)

を以下のステップで求める。

【００３７】step 1. 中間値の計算

U1=X1*Z2^2, U2=X2*Z1^2, S1=Y1*Z2^3,

S2=Y2*Z1^3, H=U2-U1, r=S2-S1

を計算する。

【００３８】step 2. R = (X3, Y3, Z3, a*Z3^4) を求める。

X3 = -H^3 -2U1*H^2+ r^2,

Y3 = -S1*H^3 + r(U1*H^2 -X3),

Z3 = Z1*Z2*H,

a*Z3^4 = a(Z3^2)^2

（実施の形態２）図２は楕円曲線演算装置における修正ヤコビアンによる2倍点の方法を示すものである。以下同図を参照しながら加算方法を説明する。

【００３９】ここでも実施の形態１と同様に、pを160ビットの素数とし、GF(p)上の楕円曲線 E:y^2 = x^3 +ax+b, その元 P=(X1, Y1, Z1, a*Z1^4) で表すとき、

2P = (X3, Y3, Z3, a*Z3^4)

を以下のステップで求める。

【００４０】step 1. 中間値の計算

S=4X1*Y1^2, M=3X1^2+a*Z1^4, T=-2S+M^2

を計算する。

【００４１】step 2. 2P = (X3, Y3, Z3, a*Z3^4) を求める。

X3 = T,

Y3 = -8Y1^4 + M(S-T),

Z3 = 2Y1*Z1,

a*Z3^4 = 2^4*(Y1^4)*(a*Z1^4)

上記の実施の形態１、２の計算量について述べる。GF(p)上の1回の乗算をMul、逆元演算をInv、2乗算をSqで表す。InvとMulの比率は、実装方法により異なるが、SqとMulの比率は、約 Sq=0.8Mul である。

【００４２】実施の形態１、２を用いて楕円曲線上の加算、2倍点を実現すると、加算が13Mul+6Sq で、2倍算は、4Mul+4Sq回で実現できる。加算は、従来から知られているプロジェクティブ座標、ヤコビアン座標、チャド

ノブスキヤコビアン座標に比較すると計算量が多いが、2倍算は、従来の座標系のどれよりも少ない計算量で実現できる。

【００４３】楕円曲線の冪倍点 kP (k=160ビット) の演算は、加算に比べ2倍算の繰り返し回数が多い。このため、従来例２にヤコビアン座標の代わりに、実施の形態１、２の修正ヤコビアン座標を用いると、高速化ができる。実際、従来例２が1882Mulで合ったのに対し、実施の形態１、２の修正ヤコビアン座標を適用すると、1722 Mulで実現できる。よって、2倍算が高速な修正ヤコビアンの効果は大きい。

【００４４】（実施の形態３）図３は本発明の実施の形態３における楕円曲線演算装置の構成を示すものである。

【００４５】以下同図を参照しながら実施の形態の手順を説明する。p を160ビットの素数とし、有限体GF(p)上の楕円曲線を E とし、E(GF(p)) の任意の元を P , k*P の計算をする。ここで、kが従来例２のように、以下で表されているとする。

【００４６】k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1]) ・・・)+W[0])

step 1. 予備計算テーブルの作成

sP(s=3,5,...,15)をアフィン座標で計算し、予備計算テーブルとする。

【００４７】step 2. kP の計算

Tを上位ビットより探索し、ウインドウがある毎に、予備計算テーブルの値(アフィン座標) との加算を修正ヤコビアン座標で求めて、その結果を修正ヤコビアン座標で2冪倍するが、最終結果はヤコビアン座標で得ることを繰り返す。

【００４８】すなわち、2^kP1 +W[2]Pを、(P1は途中の計算結果で修正ヤコビアン座標)

step 2-1. (k-1)回 、P1を修正ヤコビアン座標により2倍算する。

【００４９】step 2-2. 2^(k-1)P1 を２倍し、結果をヤコビアン座標で与える。

step 2-3. W[2]P をテーブルから参照する（アフィン座標)

step 2-4. ヤコビアン座標の 2^kP1 とアフィン座標のW[2]Pを加算し、結果は修正ヤコビアン座標で与える。

【００５０】上記実施の形態３の楕円演算装置は、2倍算においては最も計算量の少ない修正ヤコビアン座標を、加算においては、ヤコビアン座標とアフィン座標の結果を修正ヤコビアン座標で得るという混合座標を用いることにより、全体の乗算の回数を減らすことができる。実際、トータルの計算量は、8Inv+1456Mulである。従来例の1882Mulに比較して、Inv<;53.3Mul であれば実施の形態３の方が高速になる。一般に、Inv<;30Mulであることより、従来例よりはるかに高速に実現出来る。

【００５１】（実施の形態４）図４は本発明の実施の形態４における楕円曲線演算装置の構成を示すものである。

【００５２】以下同図を参照しながら本実施の形態の手順を説明する。p を160ビットの素数とし、有限体GF(p)上の楕円曲線を E とし、E(GF(p)) の任意の元を P , k*P の計算をする。ここで、kが従来例２のように以下で表されているとする。

【００５３】k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1]) ・・・)+W[0])

step 1. 予備計算テーブルの作成

sP(s=3,5,...,15)を、2Pは、アフィン座標で計算し、2P+sP をチャドノブスキヤコビアン座標で求めることにより、予備計算テーブルを作成する。

【００５４】（予備計算テーブルはチャドノブスキヤコビアン座標)

step 2. kP の計算

Tを上位ビットより探索し、ウインドウがある毎に、予備計算テーブルの値(チャドノブスキヤコビアン座標) との加算を修正ヤコビアン座標で求めて、その結果を修正ヤコビアン座標で2冪倍するが、最終結果はヤコビアン座標で得ることを繰り返す。

【００５５】すなわち、2^kP1 +W[2]Pを、(P1は途中の計算結果で修正ヤコビアン座標)

step 2-1. (k-1)回 、P1を修正ヤコビアン座標により2倍算する。

【００５６】step 2-2. 2^(k-1)P1 を２倍し、結果をヤコビアン座標で与える。

step 2-3. W[2]P をテーブルから参照する（チャドノブスキヤコビアン座標)

step 2-4. ヤコビアン座標の 2^kP1 とチャドノブスキヤコビアン座標のW[2]Pを加算し、結果は修正ヤコビアン座標で与える。

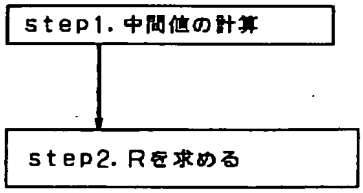
【００５７】上記実施の形態４の楕円演算装置は、2倍算においては最も計算量の少ない修正ヤコビアン座標を、加算においては、ヤコビアン座標とチャドノブスキヤコビアン座標の結果を修正ヤコビアン座標で得るという混合座標を用いることにより、全体の乗算の回数を減らすことができる。実際、トータルの計算量は、Inv+1593Mulである。従来例の1882Mulに比較して、Inv<;289Mul であれば実施の形態４の方が高速になる。一般に、Inv<;30Mulであることより、従来例よりはるかに高速に実現出来る。

【００５８】（実施の形態５）図５は本発明の実施の形態５における楕円曲線演算装置の構成を示すものである。

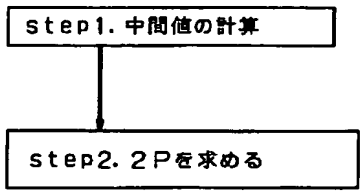
【００５９】以下同図を参照しながら本実施の形態の手順を説明する。pを160ビットの素数とし、有限体GF(p)上の楕円曲線を E とし、E(GF(p)) の任意の元を P , k*P の計算をする。ここで、kが従来例２のように以下で表されているとする。

【００６０】k=2^k0(2^k1(・・・ (2^kvW[v] +W[v-1])・・・)+W[0])
step 1. 予備計算テーブルの作成
sP(s=3,5,...,15)を、チャドノブスキヤコビアン座標で求めることにより、予備計算テーブルを作成する。
【００６１】（予備計算テーブルはチャドノブスキヤコビアン座標）
step2. kP の計算
Tを上位ビットより探索し、ウインドウがある毎に、予備計算テーブルの値(チャドノブスキヤコビアン座標)との加算を修正ヤコビアン座標で求めて、その結果を修正ヤコビアン座標で2冪倍するが、最終結果はヤコビアン座標で得ることを繰り返す。
【００６２】すなわち、2^kP1 +W[2]Pを、(P1は途中の計算結果で修正ヤコビアン座標)
step 2-1. (k-1)回 、P1を修正ヤコビアン座標により2倍算する。
【００６３】step 2-2. 2^(k-1)P1 を２倍し、結果をヤコビアン座標で与える。
step 2-3. W[2]P をテーブルから参照する（チャドノブスキヤコビアン座標）
step 2-4. ヤコビアン座標の 2^kP1 とチャドノブスキヤコビアン座標のW[2]Pを加算し、結果は修正ヤコビアン座標で与える。
【００６４】上記実施の形態５の楕円演算装置は、2倍算においては最も計算量の少ない修正ヤコビアン座標を、加算においては、ヤコビアン座標とチャドノブスキヤコビアン座標の結果を修正ヤコビアン座標で得るという混合座標を用いることにより、全体の乗算の回数を減らすことができる。実際、トータルの計算量は、1619Mulである。従来例の1882Mulに比較して、はるかに高速に実現出来る。
【００６５】
【発明の効果】以上に説明したように本発明は、従来例における問題点を鑑みて行なわれたもので、高速な暗号方式や署名方式を可能にする楕円曲線演算装置を提供することができ、その実用的価値は大きい。
【図面の簡単な説明】
【図１】本発明における実施の形態１の楕円曲線演算装置の構成図
【図２】本発明における実施の形態２の楕円曲線の演算装置の構成図
【図３】本発明における実施の形態３の楕円曲線演算装置の構成図
【図４】本発明における実施の形態４の楕円曲線の演算装置の構成図
【図５】本発明における実施の形態５の楕円曲線演算装置の構成図
【図６】従来例１のエルガマル署名の構成図
【図７】従来例２の楕円曲線演算装置を示す図

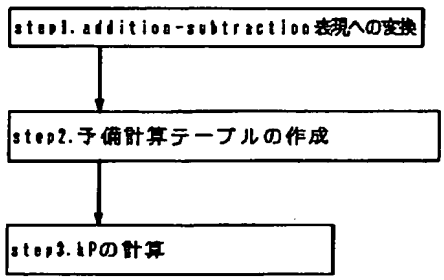
【図１】



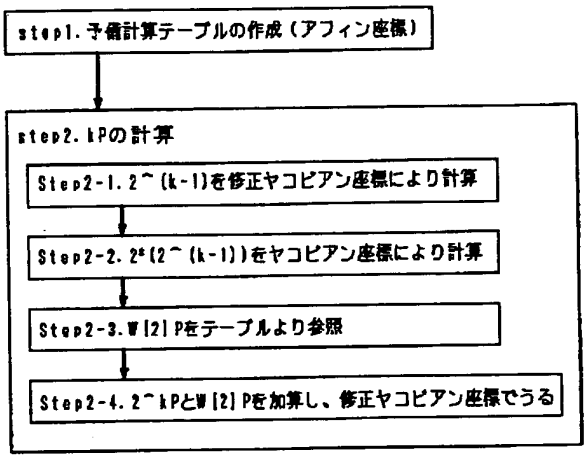
【図２】



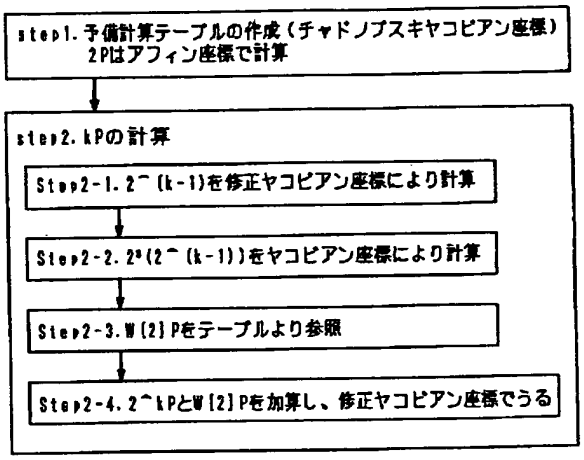
【図７】



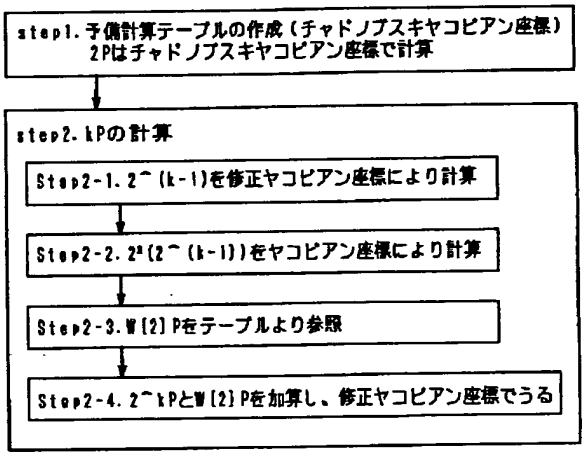
【図３】


step1. 予備計算テーブルの作成（アフィン座標）
step2. kPの計算
Step2-1. 2^(k-1)を修正ヤコビアン座標により計算
Step2-2. 2^(2^(k-1))をヤコビアン座標により計算
Step2-3. W[2]Pをテーブルより参照
Step2-4. 2^kPとW[2]Pを加算し、修正ヤコビアン座標でうる

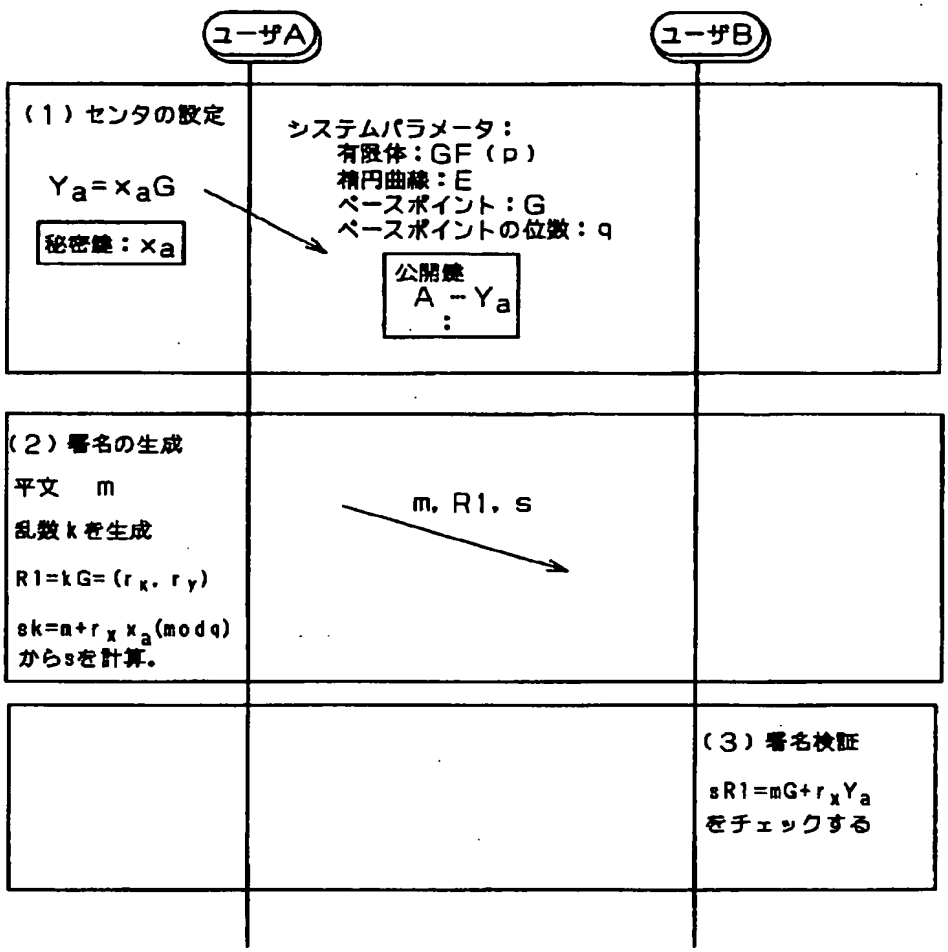
【図４】


step1. 予備計算テーブルの作成（チャドノブスキヤコビアン座標）
2Pはアフィン座標で計算
step2. kPの計算
Step2-1. 2^(k-1)を修正ヤコビアン座標により計算
Step2-2. 2^(2^(k-1))をヤコビアン座標により計算
Step2-3. W[2]Pをテーブルより参照
Step2-4. 2^kPとW[2]Pを加算し、修正ヤコビアン座標でうる

【図５】


step1. 予備計算テーブルの作成（チャドノブスキヤコビアン座標）
2Pはチャドノブスキヤコビアン座標で計算
step2. kPの計算
Step2-1. 2^(k-1)を修正ヤコビアン座標により計算
Step2-2. 2^(2^(k-1))をヤコビアン座標により計算
Step2-3. W[2]Pをテーブルより参照
Step2-4. 2^kPとW[2]Pを加算し、修正ヤコビアン座標でうる

【図６】


ユーザA
ユーザB
（１）センタの設定
$Y_a = x_a G$
秘密鍵：x_a
システムパラメータ：
有限体：GF（p）
楕円曲線：E
ベースポイント：G
ベースポイントの位数：q
公開鍵
A
Y_a
：
（２）署名の生成
平文　m
乱数kを生成
$R1 = kG = (r_x, r_y)$
$sk = m + r_x x_a \pmod q$
からsを計算。
m, R1, s
（３）署名検証
$sR1 = mG + r_x Y_a$
をチェックする